REMARKS

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 are currently pending in the subject application and are presently under consideration. Claims 1-9, 12-17, 19-21, 25, 30, 41, 46, and 48-50 have been amended as shown on pages 2-11 of the Reply. Claims 26-29 and 31-40 have been cancelled. New claims 51 and 52 has been added. Claims 10, 11, 18, 22, 24, and 42-44 were cancelled previously.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 Under 35 U.S.C. §103(a)

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 stand rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Swiler, *et al.* (US 7,013,395) in view of Townsend (U.S 6,374,358), and further in view of Godwin (US 2004/0059920). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Swiler, *et al.*, Townsend, and Godwin, individually or in combination, do not disclose or suggest all features of the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

The present application relates generally to network and automation device security in an industrial automation environment. According to one or more embodiments, a network-based security learning system (*e.g.*, a learning component) can be provided that monitors an automation network during a predetermined training period. During the training period, the

learning component can monitor and learn activities or patterns such as the number of network requests to and from one or more assets, the type of requests, status or counter data, or substantially any data type or pattern that can be retrieved from the network or asset. After the training period, the learning component can monitor the automation network or assets for detected deviations from data patterns learned during the training period. If desired, a user interface can be provided, wherein one or more pattern thresholds can be adjusted. An alarm or automated event can then occur if a deviation is detected outside the threshold (see, *e.g.*, page 5, line 11 - page 6, line 5). In particular, amended independent claim 1 recites, *a learning component that mon**itors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication**; and an analyzer component that monitors data traffic subsequent to the training period and **generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation**, the one or more security outputs including at least one output that alters the data traffic between the controller and the at least one I/O device.*

Swiler, *et al.* does not disclose or suggest at least these features. Swiler, *et al.* relates to an analysis tool that assesses potential security risks in a network. This analysis tool uses as input a database of common attacks broken into atomic steps, specific network configuration and topology information, and an attacker profile. The attack information is matched with the network configuration information and an attacker profile to create an attack graph. Graph algorithms are then applied to the attack graph to identify attack paths with the highest probability of success (see column 3, line 67 - column 4, line 11) . However, Swiler, *et al.* makes no determination as to whether a *current pattern of data traffic deviates from a learned pattern* in excess of an acceptable deviation. Indeed, Swiler, et al. does not assess a network's current access pattern for any purpose, and therefore fails to contemplate comparing such an current access pattern with a learned access pattern.

Since Swiler, *et al.* fails to disclose determining whether *a current pattern of data traffic deviates from a learned pattern in excess of an acceptable deviation*, it follows that the cited reference is also silent regarding generation of one or more security outputs that alter a current pattern of data traffic. In this regard, it is noted that the above-described attack graph is employed for informational purposes only in order to assess a risk to network assets. Since the attack graph of Swiler, *et al.* is merely employed for informational purposes, the cited reference

does not contemplate generating any type of security output, much less doing so based on whether a current access pattern deviates from a learned access pattern in excess of an acceptable deviation.

Townsend is also silent regarding these aspects. Townsend relates to a method selecting a security model for protecting an application from attack by unauthorized sources. To this end, a current countermeasure strength level and a recommended countermeasure strength level are determined for each of at least one countermeasure based on input data and security risk data. A security model including at least one countermeasure and a corresponding strength level is determined based on the current and the recommended strength levels (see column 2, lines 19-29). However, Townsend does not make a determination as to whether a *current pattern of data traffic deviates from a learned pattern*. Rather, the security model selection method of Townsend compiles business concerns, potential network attack types, and possible countermeasures, and uses this data to analyze each possible countermeasure with respect to each attack type for cost and effectiveness. None of this data entails an analysis of a *current or learned pattern* of data traffic, and consequently the cited reference makes no determination regarding whether a *current pattern of data traffic deviates from a learned pattern*.

Moreover, like Swiler, *et al.*, Townsend does not generate a security output that can alter the current access pattern, or perform a direct action of any kind on a system under analysis. With regard to outputs, Townsend merely generates a written report of the above-described assessment that includes a recommendation for countermeasure implementation (see column 8, lines 1-13). Townsend therefore fails to remedy the deficiencies of Swiler, *et al.* with regard to *generating one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation*, wherein *the one or more security outputs include at least one output that alters the data traffic between the controller and the at least one I/O device*.

Godwin does not cure the above deficiencies. Godwin relates to a tool for checking storage management system security settings. This tool accesses one or more security parameters, compares them to security policies, rules, and allowable values, and reports noncompliant settings *via* a user-readable report. According to Godwin, a set of automatic correction rules may also be employed to automatically modify noncompliant settings to bring them into compliance (see Abstract). However, these parameter checks do not involve any

manner of assessment on network access patterns generally. Rather, Godwin merely performs a check on each storage security parameter to ensure the parameter is within a compliant range. As such, Godwin fails to remedy the shortcomings of the other cited references with regard to an analyzer component that generates one or more security outputs *if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation, the one or more security outputs including at least one output that alters the data traffic between the controller and the at least one I/O device.*

Similarly, amended independent claim 12 recites, ***monitoring communication of data associated with the I/O table for a predetermined training period to learn at least one learned pattern of communication****...and performing at least one automated security event* ***if a current pattern of the data traffic deviates from the at least one learned pattern in excess of the acceptable deviation*** *after the training period.* None of Swiler, *et al.*, Townsend, or Godwin disclose or suggest performing an automated security event if a current pattern of data traffic deviates from a learned pattern in access of an acceptable deviation, as discussed *supra.* The cited references also fail to disclose learning this learned accesses pattern by *monitoring communication of data associated with the I/O table for a predetermined training period.*

Likewise, amended independent claim 16 recites, *means for* ***monitoring communication of data associated with the I/O table for a predetermined training period****; means* ***for learning at least one learned pattern of communication based on the means for monitoring****...means for automatically* ***detecting that a current pattern of communication of the data associated with the I/O table deviates from the learned pattern in excess of the acceptable deviation*** *after the training period; and means for performing an automated action that alters the current pattern of communication in response to the detecting.* As discussed above, the cited references are silent regarding these features.

Also, amended independent claim 17 recites, *a learning component that* ***monitors communication of data associated with the I/O table to and from the industrial controller during a training period and establishes a learned pattern of communication****; and an analyzer component that monitors a current pattern of communication of the data associated with the I/O table subsequent to the training period and automatically* ***performs a security action to bring the current pattern in line with the learned pattern in response to detecting that the current pattern communication has deviated from the learned pattern of access in excess of a defined***

pattern threshold. Swiler, *et al.*, Townsend, and Godwin are silent regarding these aspects, as noted previously.

Also, amended independent claim 30 recites, *means for* ***monitoring communication of data associated with the I/O table to and from the industrial controller during a training period and establishing a learned pattern of communication****...means for initiating a security procedure that* ***performs a security action to bring the current pattern in line with the learned pattern if the means for monitoring identifies that a current access pattern deviates from the at least learned pattern in excess of the allowable deviation.*** As discussed above, none of Swiler, *et al.*, Townsend, or Godwin disclose or suggest these aspects.

Amended claim 49 recites, *the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation.* As already discussed, the cited references fail to disclose performing a security action upon detection of a deviation of a current pattern of data traffic from a learned pattern in excess of an acceptable deviation. The cited references therefore fail to disclose in particular that such a security action can comprise disabling network requests from at least one outside network.

In view of at least the foregoing, it is respectfully submitted that Swiler, *et al.*, Townsend, and Godwin, individually or in combination, do not disclose or suggest all aspects of amended independent claims 1, 12, 16, 17, and 30 (and all claims depending there from), and as such fail to render obvious the present application. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731